UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,655	03/01/2004	Naohiro Tamura	1503.69885	9572

7590 12/20/2007

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
12/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/790,655	Applicant(s) TAMURA ET AL.
	Examiner Andrew L. Nalven	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 November 2007</u>.

2a)☐ This action is **FINAL.** 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 5-26* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 5-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>01 March 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-2, 5-26 are pending.

Response to Arguments

2.   Applicant's arguments filed 11/5/2007 regarding the rejections under §101 have

been fully considered but they are not persuasive. Applicant's remaining arguments are

moot in view of the new grounds of rejection.

3.   Applicant has argued on page 12 against the §101 rejection of claim citing *State*

Street as support for their being a useful, concrete, and tangible result. Examiner

respectfully disagrees. *State Street* is distinguishable from the instant claims because

the in *State Street* the claims were directed to the practical application of an abstract

idea. In the present case there is no practical application of the abstract idea because

the claimed system may be interpreted as purely software. Given its broadest

reasonable interpretation, claim 1 could be interpreted as purely software and thus it

fails to fall into one of the 4 classes of statutory inventions defined by § 101.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

1.   **Claims 1 and 27 are rejected under 35 U.S.C. 101** because the claimed

invention is directed to non-statutory subject matter.

2.   **Regarding claim 1,** the claim is directed towards nonstatutory subject matter.

The cited claim is an example of functional descriptive material consisting of data

structures and programs that impart functionality when employed as executed by a

computer component. Given its broadest reasonable interpretation, claim 1 could be

interpreted as purely software and thus it fails to fall into one of the 4 classes of

statutory inventions defined by § 101.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   **Claims 1-2, 5-9, 12-18, and 22-26 are rejected under 35 U.S.C. 103(a)** as

being unpatentable over Talpade et al US PGPub 2004/0148520 in view of Tovander

US Patent No. 6,715,083.

5.   **With regards to claims 1, 13, 18, 26**, Talpade teaches an unauthorized access

prevention system (Talpade, Abstract, when attack is detected, mitigate the attack),

including: a search unit searching the flowing-in path of unauthorized access to services

disclosed from a user's communication network (Talpade, paragraph 0017, sensor 204

detects an attack, traffic entering the customer network); a determination unit

determining a place to implement a countermeasure for protecting the services from the

unauthorized access based on the result of the search (Talpade, paragraph 0024,

automatically mitigates attack by informing affected edge routers). Talpade fails to

teach a notification unit notifying, according to a determination that the countermeasure

is implemented in the flow source that makes the unauthorized access flow into the

user's communication network, the determination to a flow source. However, Tovander

teaches a notification unit notifying, according to a determination that the

countermeasure is implemented in the flow source that makes the unauthorized access

flow into the user's communication network, the determination to a flow source

(Tovander, column 3 lines 3-20 and 38-54). At the time the invention was made, it

would have been obvious to a person of ordinary skill in the art to utilize Tovander's

method of notifying a flow source because it offers the advantage of allowing servers

downstream from a source to make risk determinations when determining whether to

accept or reject packets from a particular source and allows the thwarting of a potential

hacker in real time (Tovander, column 2 line 60 – column 3 line 40).

6.   **With regards to claim 2,** Talpade as modified teaches a recording medium in

which a program that directs a computer to implement a countermeasure against

unauthorized access is recorded and in which the program can be read by the

computer, and the program directs the computer to perform the following processes by

being executed by the computer (Talpade, paragraph 0019, host platform): a search

process of searching the flowing-in path of the unauthorized access to the services

disclosed from the user's communication network (Talpade, paragraph 0017, sensor 204 detects an attack, traffic entering the customer network); a determination process of determining the place to implement the countermeasure for protecting the services from the unauthorized access based on the result of the search (Talpade, paragraph 0024, automatically mitigates attack by informing affected edge routers); and a notification process of notifying, according to a determination that the countermeasure is implemented in the flow source that makes the unauthorized access flow into the user's communication network, the determination to the flow source (Talpade, paragraph 0024, new routing information is sent to the border and edge routers).

7.   **With regards to claim 5**, Talpade as modified teaches the process of searching the flowing-in path is performed by the computer based on the monitoring information on the traffic transmitted by a user's communication network and the unauthorized access information indicating the contents of the unauthorized access (Talpade, paragraph 0020, searching is based upon all traffic entering customer network, searching looks at information in headers – sensor two).

8.   **With regards to claim 6**, Talpade as modified teaches the monitoring information includes at least the position information on an edge router arranged on the border between the user's communication network and the communication network adjacent to the user's communication network and the monitoring information on the traffic that flows into the user's communication network via the edge router (Talpade, paragraph 0020, position information - monitors all traffic entering a particular

customers network, paragraph 0024, informs all border/edge routers for the customer

network to reroute traffic).

9.   **With regards to claim 7** (as best understood), Talpade as modified teaches the

process of notifying the determination to the flow source after mutual attestation is

conducted between the notification unit and the flow source of the unauthorized access

is performed by the computer (Talpade, paragraph 0024, new routing information is sent

to border/edge routers).

10.   **With regards to claim 8**, Talpade as modified teaches the process of notifying

the determination to the flow source after information on a security policy for the

operation of each network is exchanged with the flow source that transmits the

unauthorized access is performed by the computer (Talpade, paragraph 0024, security

policy in the form of new routing information is sent to border/edge routers).

11.   **With regards to claim 9**, Talpade as modified teaches information on a security

policy is the information indicating the time required till the countermeasure against the

unauthorized access is cancelled after the unauthorized access is not detected any

more (Talpade, paragraph 0028, periodic polling to determine if attack has completed).

12.   **With regards to claim 12**, Talpade as modified teaches the process of notifying

the flow source of the unauthorized access of the determination using the

communication path that differs from the flowing-in path of the unauthorized access is

performed by the computer (Talpade, paragraph 0023, notification is provided through

IP tunnels).

13.   **With regards to claim 14,** Talpade as modified teaches the judgment is made

based on the judgment information on the flow source that is given in advance

(Talpade, paragraph 0020, judgment whether to send notification determined from

sensor findings in advance of sending notification).

14.   **With regards to claim 15,** Talpade as modified teaches that by having the

program executed by the computer; the unauthorized access countermeasure

implementation control process that has the countermeasure for protecting the services

from the unauthorized access implemented in the user's communication network based

on the determination that said countermeasure is implemented in the user's

communication network is performed by the computer (Talpade, paragraph 0024,

implemented by analysis engine and filter router).

15.   **With regards to claim 16,** Talpade as modified teaches the process of

implementing the countermeasure in the POP (point of presence) edge router to which

the flow source of the unauthorized access is connected is performed by the computer

(Talpade, paragraph 0024, new routing information is sent to border/edge routers).

16.   **With regards to claim 17,** Talpade as modified teaches the process of

identifying the POP edge router to which the transmitter that transmits the unauthorized

access is connected based on the information obtained from the operation management

system that manages the operation of the user's communication network is further

performed by the computer (Talpade, paragraph 0024, analysis engine/ISP

manager/filter routers determine provide new routing tables to mitigate attack).

17.   **With regards to claim 22,** Talpade teaches that by having the program

executed by the computer; the process-of obtaining a notification of the determination

that unauthorized access to the services disclosed from a communication network

different from the user's communication network is made to flow into said other

communication network is performed by the computer (Talpade, paragraph 0017,

sensor 204 detects an attack, traffic entering the customer network); the process of

searching the flowing-in path of the unauthorized access related to the notification in the

user's communication network when the notification is obtained by the notification

obtaining process is performed by the computer (Talpade, paragraph 0017, sensor 204

detects an attack); the process of determining the place to implement the

countermeasure for protecting the services disclosed from said other communication

network from the unauthorized access related to the notification based on the result of

the search when the notification is obtained by the notification obtaining process is

performed by the computer (Talpade, paragraph 0024, analysis engine/ISP

manager/filter routers determine provide new routing tables to mitigate attack). Talpade

fails to teach and the process of notifying, according to a determination that the

countermeasure is implemented in the flow source that makes the unauthorized access

related to the notification flow into the user's communication network when the

notification is obtained by the notification obtaining process, the determination to the

flow source is performed by the computer. However, Tovander teaches and the

process of notifying, according to a determination that the countermeasure is

implemented in the flow source that makes the unauthorized access related to the

notification flow into the user's communication network when the notification is obtained

by the notification obtaining process, the determination to the flow source is performed

by the computer (Tovander, column 3 lines 3-20 and 38-54). At the time the invention

was made, it would have been obvious to a person of ordinary skill in the art to utilize

Tovander's method of notifying a flow source because it offers the advantage of

allowing servers downstream from a source to make risk determinations when

determining whether to accept or reject packets from a particular source and allows the

thwarting of a potential hacker in real time (Tovander, column 2 line 60 – column 3 line

40).

18.   **With regards to claim 23**, Talpade as modified teaches that by having the

program executed by the computer; the unauthorized access countermeasure

implementation control process that has the countermeasure for protecting the services

disclosed from the user's communication network or the other communication network

from the unauthorized access related to the notification implemented in the

communication network of the notification source of the notification when the notification

obtained by said notification obtaining process is the same as that obtained in the past

is further performed by the computer (Talpade, paragraph 0024, countermeasures for

all attacks created by implementing new routing information that is sent to the border

and edge routers).

19.   **With regards to claim 24**, Talpade as modified teaches the process of notifying

the information that uniquely identifies the unauthorized access related to the

notification when the determination is notified is performed by the computer (Talpade, paragraph 0022, notification of attack is sent by sensor).

20.   **With regards to claim 25**, Talpade as modified teaches having the program executed by the computer; the process of recording the history of the notification is further performed by the computer (Talpade, paragraph 0028, record of notifications stored such that analysis engine can later determine if the attack is completed).

21.   **Claims 10-11, 19-21 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Talpade et al US PGPub 2004/0148520 and Tovander US Patent No. 6,715,083, as applied to claim 1 and 13 above, and in further view of Kaler et al US PGPub 2004/0003286.

22.   **With regards to claim 10** (as best understood), Talpade fails to teach that the time indicated by the information on the security policy differs between the user communication network and the flow source, a shorter time of the two is used as the time required till the countermeasure against unauthorized access is cancelled after the unauthorized access is not detected any more. However, Kaler teaches that the time indicated by the information on the security policy differs between the user communication network and the flow source, a shorter time of the two is used as the time required till the countermeasure against unauthorized access is cancelled after the unauthorized access is not detected any more (Kaler, paragraph 0036, time period for countermeasures if predefined in the threat source). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kaler's method of timing countermeasures because it offers the advantage of increasing

security and efficiency by allowing a countermeasure's time of enactment to be dependent upon the severity of the attack (Kaler, paragraph 0036).

23.   **With regards to claim 11,** Talpade as modified teaches the process of notifying the flow source of the determination and the information indicating the time required till the countermeasure against the unauthorized access is cancelled after the unauthorized access is not detected any more is performed by the computer (Kaler, paragraph 0036, time period for countermeasures if predefined in the threat source, paragraph 0021, computer device).

24.   **With regards to claim 19,** Talpade teaches the countermeasure implemented by the unauthorized access countermeasure implementation control process is cancelled after the unauthorized access is not detected any more (Talpade, paragraph 0028, determine when the attack is completed), but fails to teach a preset time. However, Kaler teaches a preset time for cancellation of countermeasures (Kaler, paragraph 0036, time period for countermeasures if predefined in the threat source). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kaler's method of timing countermeasures because it offers the advantage of increasing security and efficiency by allowing a countermeasure's time of enactment to be dependent upon the severity of the attack (Kaler, paragraph 0036).

25.   **With regards to claim 20,** Talpade as modified teaches the preset time is set based on the security policy on the network operation of both the user's communication network and the other communication network (Kaler, paragraph 0036, time period for countermeasures if predefined in the threat source depending on severity of the threat).

26.   **With regards to claim 21**, Talpade as modified teaches that when the times set

between the user's communication network and the other communication network

based on the security policy on the network operation of both networks differ between

both networks, the countermeasure is cancelled after the unauthorized access is not

detected any more and a shorter time of the two passes (Talpade, paragraph 0028,

determine when the attack is completed, Kaler, paragraph 0036, time period for

countermeasures if predefined in the threat source).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L. Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven